



Playing Devil's Advocate

A Talk About Red Teaming



Steve Keating

DATACOM



DATACOM



Why this talk?



Goal 1

Raise the profile of Red Teaming operations as a means of promoting the uptake of IT security

Goal 2

Illustrate the benefits, challenges, and potential pit falls from both the client and service providers perspective.

Why this talk?



"People only accept change when they are faced with necessity, and only recognize necessity when a crisis is upon them." — Jean Monnet

DATACOM

What is Red Teaming?



We emulate a 'crisis' so the client is more willing to accept change.

DATACOM

What is Red Teaming?



Originally a military concept

DATACOM

What is Red Teaming?



A form of penetration testing
(Strictly speaking)

DATACOM



A simulated attack against a client's network, from the Internet, to assess the security posture of that network

DATACOM



Focusing on the operational environment rather than a specific system

DATACOM

Why use it?



Demonstrate harm. Get Senior buy in. Promote improvements to security culture.

DATACOM

What it's *not*



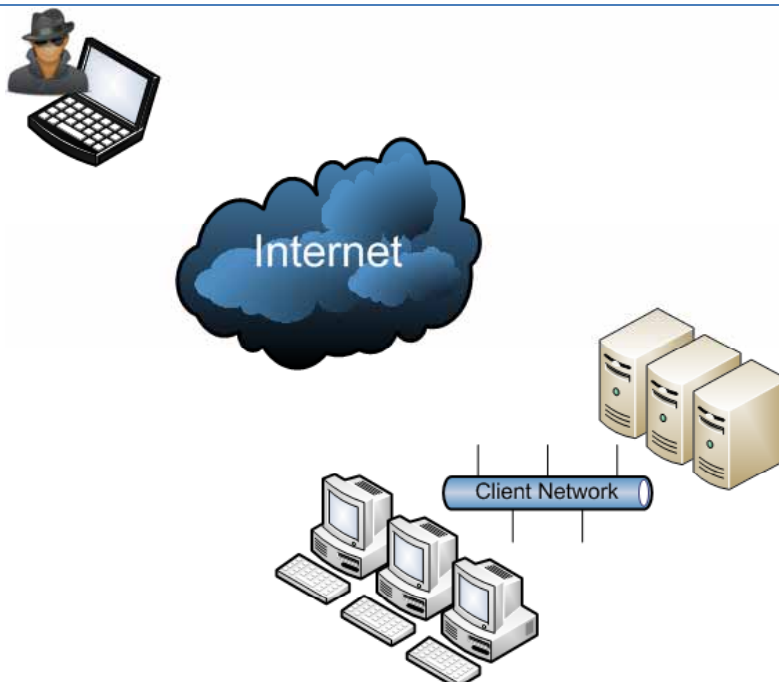
Red Teaming is **not** a substitute for a network vulnerability assessment. Especially if the client is already quite security conscious.

DATACOM



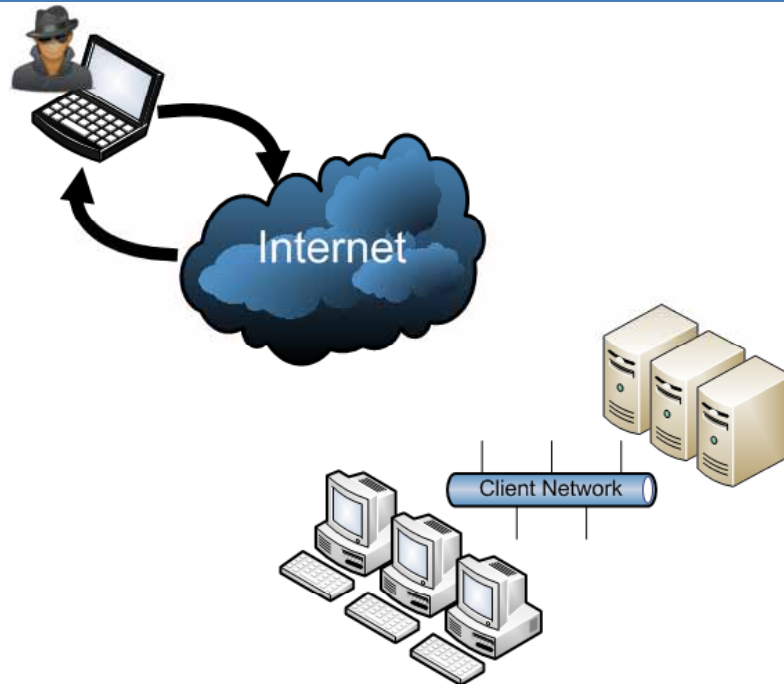
1. Recon
2. Access
3. Persistence
4. Privilege Escalation
5. Propagation
6. Exfiltration
7. Noise Escalation

DATACOM



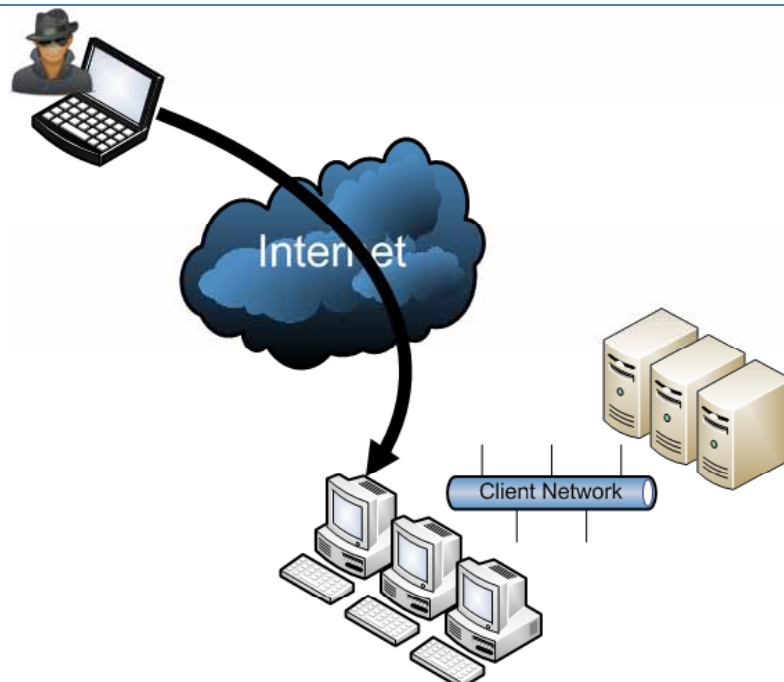
DATACOM

Methodology - Recon



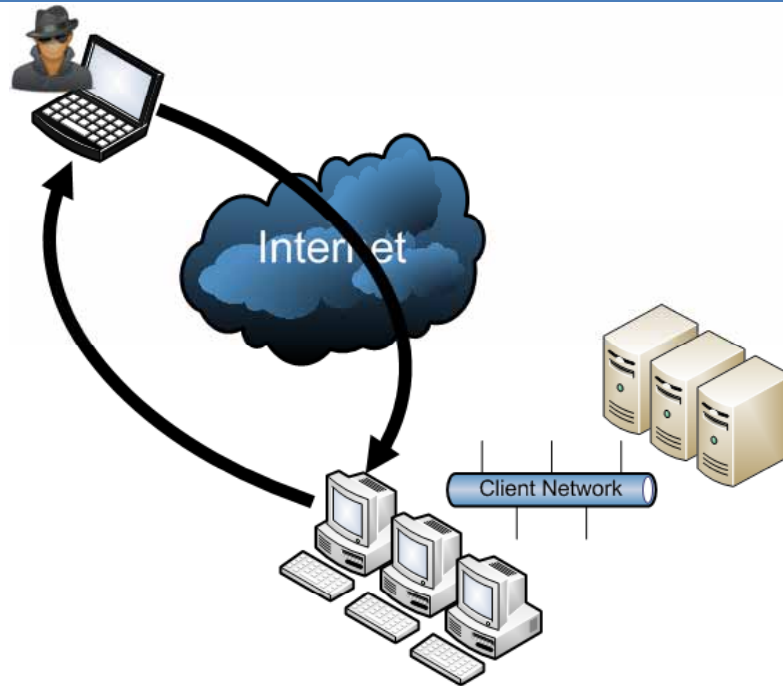
DATACOM

Methodology - Access



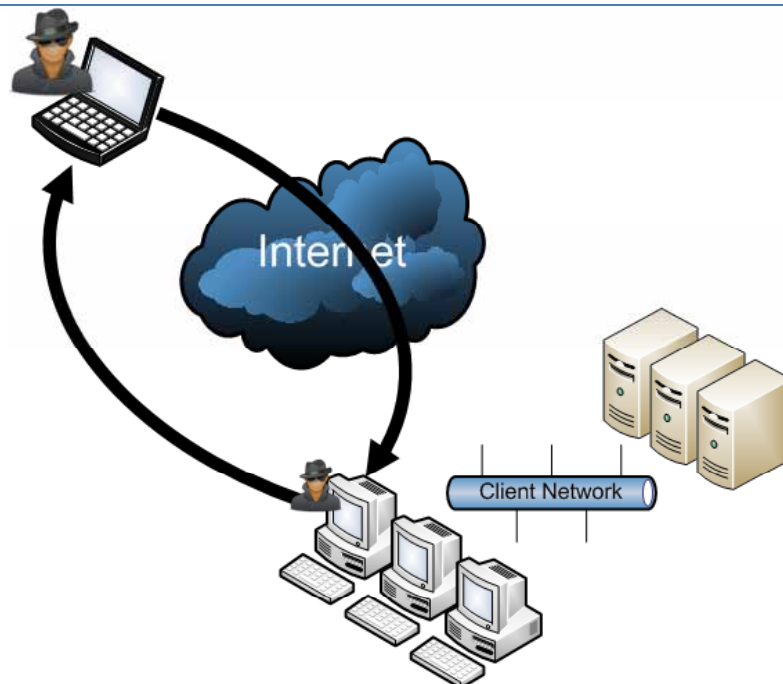
DATACOM

Methodology - Access



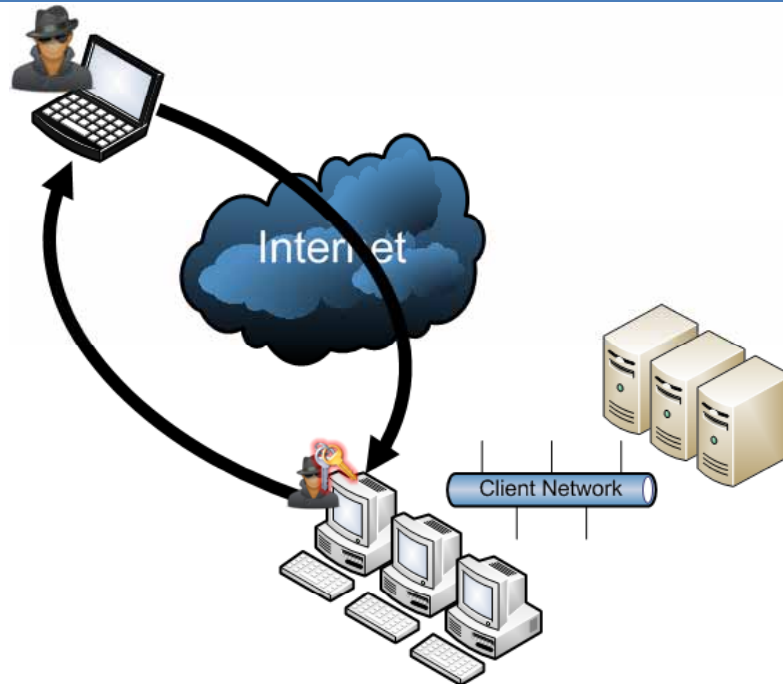
DATACOM

Methodology - Persistence



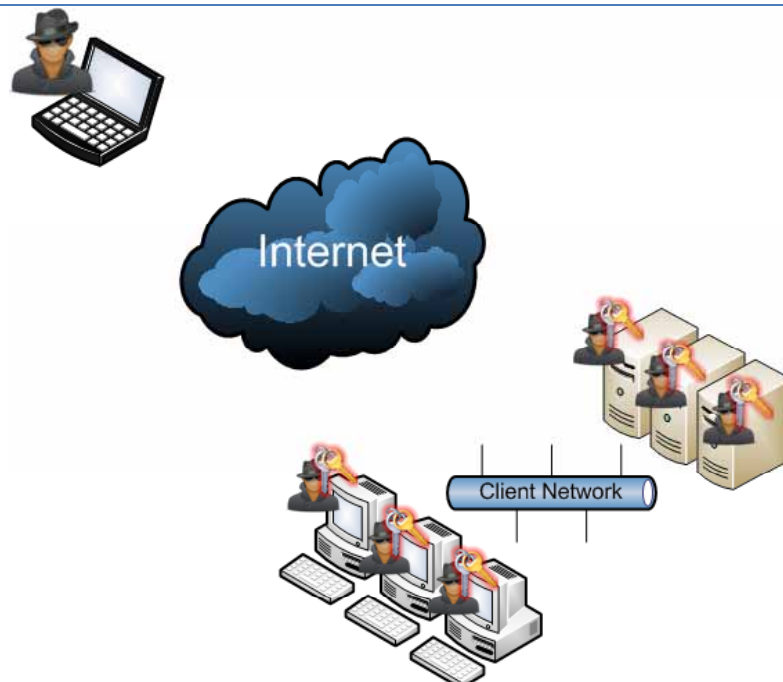
DATACOM

Methodology - Privilege Escalation



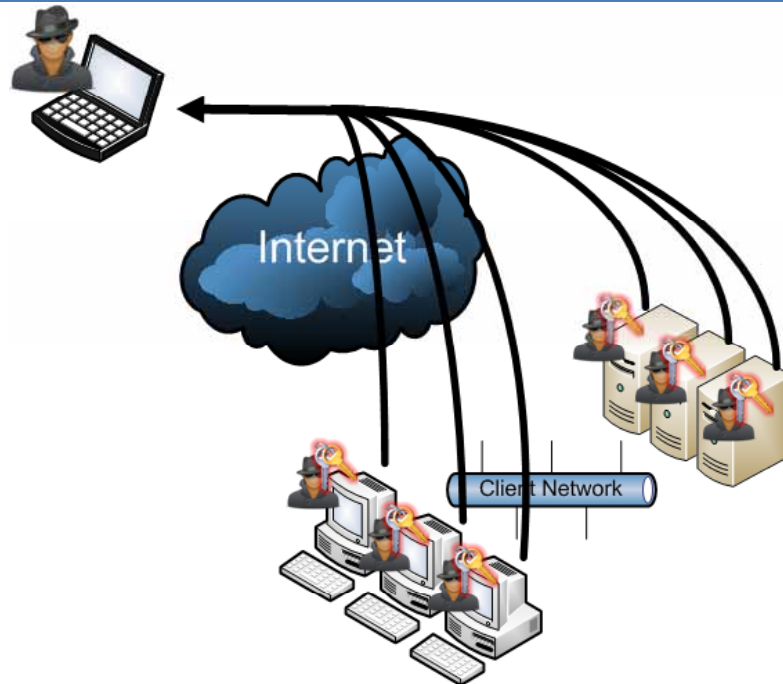
DATACOM

Methodology - Propagation



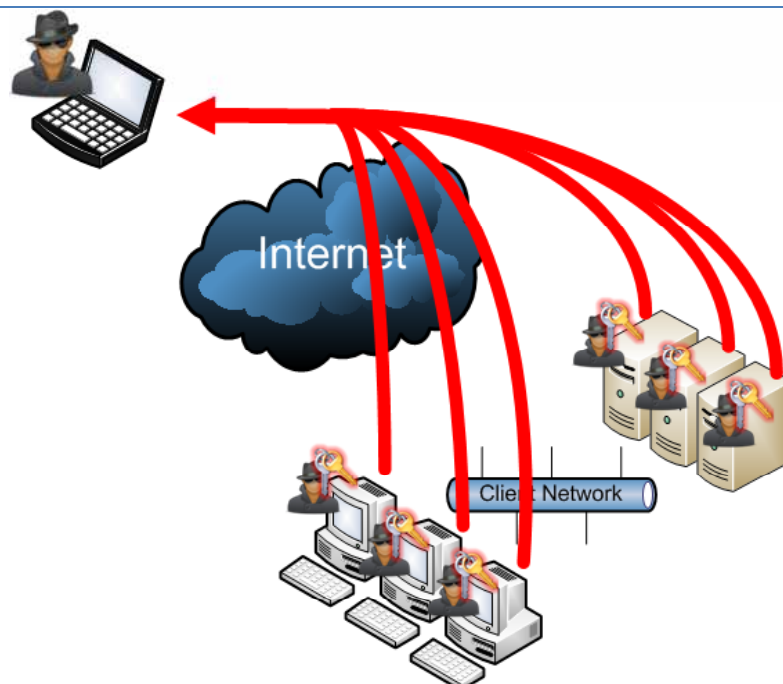
DATACOM

Methodology - Exfiltration



DATACOM

Methodology - Noise Escalation



DATACOM



Recon is obviously necessary to make sure you target the right network!

DATACOM



But don't overdo it!

DATACOM



To: HR.Department@client.com.au

From: John.Applicant@gmail.com

Subject: Job application Ref #1234

Attachments: John Applicant resume.pdf

DATACOM



To: HR.Department@client.com.au

From: John.Applicant@gmail.com

Subject: Job application Ref #1234

Attachments: **John Applicant resume.pdf**

Would you expect your HR department to open
the attachment?

DATACOM



There are many ways to gain initial 'access', but
this isn't a 'how to hack' talk...

DATACOM



"I don't care if my network has been
compromised, as long as it doesn't affect my
uptime"

DATACOM

Demonstrating the threat



Really?

DATACOM

Demonstrating the threat



Find out what they *do* care about...

DATACOM

Demonstrating the threat



... ask them!

DATACOM

Demonstrating the threat



Ask your client what it is they care about the most. This is what you will attack.

DATACOM



Why not just do a vulnerability assessment?

DATACOM



Why not just do a vulnerability assessment?

The client needs an impetus to change

DATACOM

Demonstrating the threat



Why are organisations still being compromised?

DATACOM

Exploiting the trust environment



You need to trust your users.

DATACOM



You need to trust your users.

But in a targeted attack, the attacker *becomes* the user...

DATA COM



... and detecting that a user isn't who they say they are is hard

DATA COM



What about monitoring systems?

DATACOM



Should I give up on monitoring?

DATACOM



Attacking a host without host based security?
Too easy.

DATACOM



Attacking a host with DSD's top 5 security
mitigations?
Difficult.

DATACOM



Red teaming can also show you what you're doing wrong.

DATACOM



If you control the network, you can beat the two factor authentication scheme.

DATACOM



If you control the network, you can beat the two factor authentication scheme.

DATACOM



Any authentication mechanisms are not secure across the network if the host has been compromised.

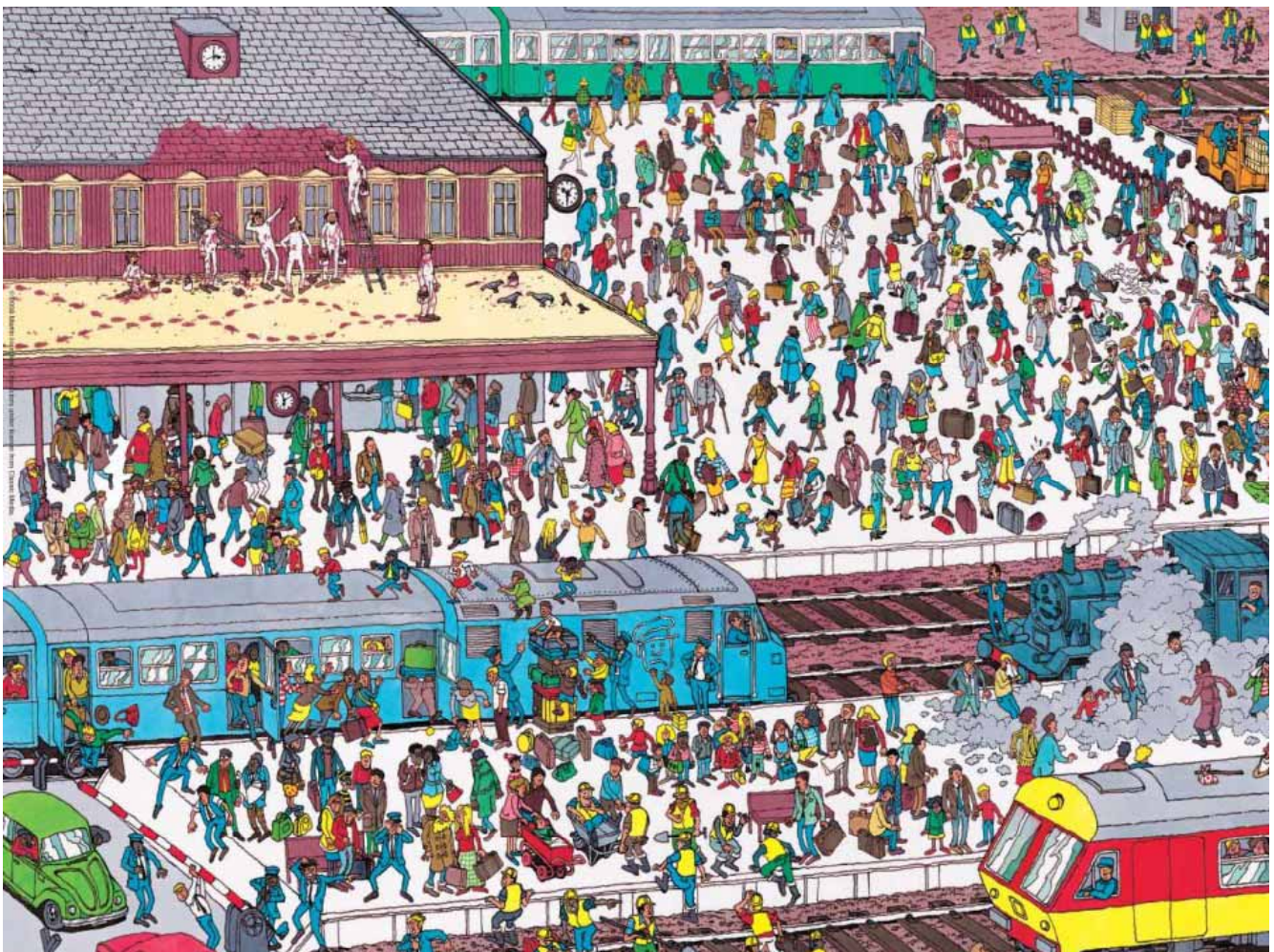
DATACOM



The big questions...

- Can we clean up?
- How well can we clean up?

DATACOM





Using a Red Teaming service as a war game scenario allows you to test all these things without wasting resources.

DATACOM



Two scenarios:

- Client detects the red team mid-op
- Red team finishes or goes to escalation phase, client attempts clean-up

DATACOM



Legal

- Approval – obviously
- Report criminal activity to police
- Report breaches of policy to client

DATACOM



Privacy

- No impersonating
- Custom or trusted software

DATACOM



You need a sound de-confliction process
Beware changes in management

DATACOM



Logging and audit trails are essential

DATACOM



Avoid the blame game

DATACOM



Avoid the blame game

DATACOM



The report should encourage the client to
embrace a security mindset,
So speak the client's language

DATACOM



Demonstrate harm.
Promote improvements to security culture.
Test incident response capability.
Provide the client with real value.

DATACOM

Thank You



DATACOM